## REMARKS

The Office Action mailed August 22, 2006 has been reviewed and carefully considered. No new matter has been added.

Claims 1-7 are pending.

Claims 1-7 stand rejected under 35 U.S.C. §103(a) as being unpatentable over SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998 (hereinafter "Stallings") in view of Diffie-Helman Key Exchange, Michael C. StJohns, Internet-Draft, 1998 (hereinafter "StJohns").

It is respectfully asserted herein that Claim 1, and all of the claims that depend there from, are patentable and non-obvious over the cited references for at least two reasons as set forth herein. First, it is respectfully asserted that none of the cited references, either taken singly or in combination, teach or suggest all of the recited limitations of Claim 1. Second, it is respectfully asserted that even assuming arguendo that all of the recited limitations are taught, the rejection must be withdrawn because the invention recited in Claim 1 would change the principle of operation of Stallings, which is a prohibition against a reference being used against a pending claim as provided in MPEP §2143.01.

Prior to furthering the above arguments, a brief description of Stalling will be provided. Stallings discloses a process referred to as key localization, which is "[t]he process by which a single user key is converted into multiple unique keys, one for each remote SNMP engine" (Stallings, p. 12, col. 2). As is shown in Figure 7 of Stallings, a user password is input to a hash function, which takes a hash of the expanded password string and outputs a user key. Then, for each remote SNMP engine, the user key is input to a hash function that takes a hash of the user key and the remote EngineID of the corresponding remote engine to output a localized key. That is" a single user key is mapped by means of a nonreversible one-way function (i.e., a secure hash function) into different localized keys for different authenticated engines (different agents)" (Stallings, p. 12, col. 2 to p. 13, col. 1). Stallings further discloses that "[a] localized key is defined ... as a secret key shared between a user and one authoritative SNMP engine" (Stallings, p. 12).

Regarding the first assertion above, none of the cited references teach or suggest the following limitations of Claim 1:

utilizing a Diffie-Hellman key exchange protocol by the SNMP manager and the SNMP agent to enter an initial privacy key and an initial authentication key into the SNMPv3 device,

wherein said utilizing step includes:

generating an associated random number and public value by both the SNMP manager and the SNMP agent;

passing the public value of the SNMP manager to the SNMP agent in a configuration file;

reading, by the SNMP manager, the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent;

computing a shared secret, by the SNMP agent and the SNMP manager, using the Diffie-Hellman key exchange protocol;

converting the shared secret into a readable password;

converting the readable password into a secret key; and

setting the initial authentication key and the initial privacy key to the value of the secret key.

For example, regarding the step of "generating an associated random number and public value by both the SNMP manager and the SNMP agent" recited in Claim 1, in the Office Action, the Examiner has cited page 12, column 1 to page 13, column 1 of Stallings and highlighted "localized keys for agent; user keys; SHA-1; HMAC" as corresponding to the associated random number and public value respectively generated by the SNMP manager and the SNMP agent (Office Action, p. 3). Regarding the limitation of Claim 1, it is noteworthy that each of the entities, namely the SNMP manager and the SNMP agent, generate respective random numbers and public values. Regarding Stallings, SHA-1 simply refers to a particular Secure Hash Algorithm and HMAC simply refers to Hashed Message Authentication Code. Accordingly, the SHA is neither a random number nor a public value, but rather a hash process. The localized key is only generated at the agent, as shown in Figure 7 of Stallings. As there is only one user key, it can only be generated by one of the manager OR the agent, and not both as per Claim 1. Even in the case where two user keys are generated, one for authentication and one for encryption, the same entity in Stallings would nonetheless generate the two user keys, and

not a manager AND an agent as per Claim 1. Thus, this step is not taught or suggested by Stallings.

Moreover, regarding the step of "passing the public value of the SNMP manager to the SNMP agent in a configuration file" recited in Claim 1, in the Office Action, the Examiner has cited page 13, column 1 of Stallings and has highlighted "configuring localized key on agent's system in secure fashion". However, the cited section of Stallings does not mention or even remotely suggest a configuration file, let alone the use of a configuration file to pass the public value of the SNMP manager to the SNMP agent as essentially recited in Claim 1. Moreover, the localized key would NOT need to be passed to the SNMP agent (remote SNMP engine) in Stallings, since it is the SNMP agent itself that locally generates the localized key (so it would essentially be passing the localized key to itself). Based on the preceding, Stallings can be considered to teach away from this step. Thus, this step is NOT taught or suggested by Stallings.

Further, regarding the step of "reading, by the SNMP manager, the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent" recited in Claim 1, in the Office Action, the Examiner has cited page 12, column 2 and has highlighted "unique key for authorized users" (Office Action, p. 3). However, in Figure 7 of Stallings, to the left of the user key may be considered one entity such as the SNMP manager, while to the right of the user key may be considered another entity(ies) such as the remote SNMP engine(s), with the user key be sent from the left entity to the right entity(ies). Accordingly, the SNMP agent on the right only receives the user key from the left side entity. Moreover, given that the remote engines locally generate the localized keys using the user key, a hash function, and a corresponding remote EngineID, there would be NO need to read a public value or any value by the SNMP manager, once the remote engines have the user key (which is not unique but rather is passed to each remote engine). Thus, this step is NOT taught or suggested by Stallings.

Moreover, regarding the step of "computing a shared secret, by the SNMP agent and the SNMP manager, using the Diffie-Hellman key exchange protocol" recited in Claim 1, in the Office Action, the Examiner has cited page 12, column 2 of Stallings and has highlighted "shared secret key" (Office Action, p. 3). However, Stallings explicitly discloses that "a localized key is defined ... as a secret key shared between a user and one authoritative SNMP engine" (Stallings, p. 12, col. 2). Since the claim limitation recites that the secret is shared by

the SNMP agent and the SNMP manager, while Stalling discloses that the secret is shared by a user and an SNMP engine, this step is NOT taught or suggested by Stallings.

Moreover, regarding the step of "converting the shared secret into a readable password" recited in Claim 1, in the Office Action, the Examiner has cited the following: "Figure 7, element: expended hashed password string; page 12, column 1, lines 29-48; human readable password; concatenating and repeating the user's password to itself to generate digest0; generating digest0 from the password; page 12, column 2, lines 29-40; 'actual secret' shared between users and authoritative SNMP engine; single user's key' the Examiner interprets such 'expended password string' or 'digest0' or 'digest1' as claimed readable password because of their similar features" (Office Action, p. 4). However, the Examiner's use of Stallings is believed to be technically improper in that it is taking the teachings of Stalling completely out of sequence in a manner contrary to the proper operation of Stallings. For example, the Examiner has already cited the use of the password and localized key with respect to previous claim limitations mentioned above, where Stallings teaches that the password is used to obtain the user key and then the user key is used to obtain the localized key, essentially represented by the following sequence: password ->(hash)-> user key ->(hash with remote EngineID)->localized key(s). However, for the present limitation being argued, the Examiner is going back to reuse the password that was previously used to obtain the user key in the first place. However, by again citing the password against this limitation, the Examiner is essentially proposing that the password that was initially input into a process to ultimately obtain the localized keys is then later output again from that same process. This clearly seems incorrect as one would not start with an input (the password), and go through a series of computationally intensive steps (hash functions) to only arrive at the same input (the password), as the Examiner is essentially suggesting. Thus, this step is NOT taught or suggested by Stallings.

The same reasoning applies to the next limitation of Claim 1, namely "converting the readable password into a secret key", as the Examiner has again used a previously obtained element (the localized key), which should have been converted into a readable password by the previous step and into a secret key in this step to follow Claim 1, which it clearly does not. Thus, this step is NOT taught or suggested by Stallings.

Returning to the second assertion, the following text of MPEP §2143.01 is provided:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (Claims were directed to an oil seal comprising a bore engaging portion with outwardly biased resilient spring fingers inserted in a resilient sealing member. The primary reference relied upon in a rejection based on a combination of references disclosed an oil seal wherein the bore engaging portion was reinforced by a cylindrical sheet metal casing. Patentee taught the device required rigidity for operation, whereas the claimed invention required resiliency. The court reversed the rejection holding the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.).

Here, Stalling discloses the generation of a user key, for example, by an SNMP manager, where the user key is then provided to each remote SNMP engine which hashes the user key with its own remote EngineID to obtain a localized key. That is, in Stallings, the SNMP manager generates a user key, and the SNMP agent hashes the user key with a remote EngineID to obtain a respective localized key. In contrast, Claim 1 recites the use of the Diffie-Helman key exchange protocol.

Accordingly, each of the entities, namely the SNMP manager (user key generation side) and the SNMP agent would require a substantial reconstruction and redesign to *possibly* be able to operate as the elements recited in Claim 1. That is, given the different approach disclosed in Stallings versus the claimed invention, each of the entities in Stallings would require a very substantial reconstruction and redesign to be able to implement the Diffie-Helman key exchange protocol in accordance with Claim 1 .

Moreover, the principle of operation of Stallings is essentially disclosed therein as follows: "a single user key is mapped by means of a nonreversible one-way function (i.e., a secure hash function) into different localized keys for different authentication engines (different agents)" (Stallings, p. 12, col. 2 to p. 13, col. 1). However, the application of the

Diffie-Helman key exchange protocol to the teachings of Stallings would completely obviate the need for the nonreversible one-way secure hash function, as well as the mapping of a single user key into different localized keys, thereby changing the principle of operation of the key localization method disclosed in Stallings. Accordingly, Stallings is improperly applied to the pending Claims per MPEP §2143.01.

While Stallings was primarily relied upon by the Examiner to reject Claim 1, it is respectfully asserted that StJohns does not cure the deficiencies of Stallings, and is silent with respect to the above-recited limitations of Stallings.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art" (MPEP §2143.03, citing *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)). Accordingly, independent Claim 1 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above.

"If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

Claims 2-7 depend from Claim 1 or a claim which itself is dependent from Claim 1 and, thus, includes all the elements of Claim 1. Accordingly, Claims 2-7 are patentably distinct and non-obvious over the cited reference for at least the reasons set forth above with respect to Claim 1.

Accordingly, reconsideration of the rejections is respectfully requested.

In view of the foregoing, Applicants respectfully request that the rejection of the claims set forth in the Office Action of August 22, 2006 be withdrawn, that pending claims 1-7 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicants' Deposit Account No.07-0832.

Respectfully submitted,

Patent Operations
Thomson Licensing Inc.
P.O. Box 5312
Princeton, NJ 08543-5312

By: /Guy H. Eriksen/
Guy H. Eriksen, Attorney for Applicants
Registration No.: 41,736
(609) 734-6807